U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

October 2024 Supplementary Examinations

rogramme: B.E. **Semester: IV**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 23CS4ESCRP **Max Marks: 100**
Course: Cryptography

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

SUPPLEMENTARY EXAMS 2024

		UNIT - I	***CO***	***PO***	**Marks**
1	a)	Analyze the following requirements and identify which security goals are addressed in each of the following cases. Provide justification for each goal identified. a. A healthcare system requires doctors to use biometric authentication to access patient records. b. An online examination system automatically logs students out after 30 minutes of inactivity. c. An e-commerce platform encrypts customer payment information during transmission. d. A financial institution maintains multiple redundant servers to ensure continuous access to online banking services.	*CO2*	*PO2*	**6**
	b)	Find the multiplicative inverse of 17 modulo 133 using the Extended Euclidean Algorithm.	*CO2*	*PO2*	**6**
	c)	Encrypt the message "attack" using the Hill cipher with the key matrix $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$. Show the steps of encryption.	*CO1*	*PO1*	**8**
		OR			
2	a)	Explain a field with example and distinguish between an infinite field and a finite field.	*CO1*	*PO1*	**8**
	b)	Use a brute-force attack to decipher the following message. Assume that you know it is encrypted using an Affine cipher and that the plaintext "ab" is enciphered to "IL". The encrypted message is " eqqtaqbvuve". a. What are the possible values for the Affine cipher key parameters K_1 and K_2? b. Decrypt the encrypted message using each possible key combination to obtain the plaintext.	*CO2*	*PO2*	**4**
	c)	Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$.	*CO1*	*PO1*	**8**

			UNIT-II			
	3	a)	Create a linear feedback shift register with 4 cells in which $b_4 = b_1 \oplus b_0$. Show the value of output for 1st 20 transitions (shifts) if the seed is $(1110)_2$.	***CO1***	***PO1***	**8**
		b)	Design a pseudocode/algorithm for the AES-128 key-expansion routine.	***CO2***	***PO2***	**6**
		c)	Compare and contrast DES and AES. Discuss the security strengths and weaknesses of DES and AES. Analyze the performance of DES and AES in terms of speed and computational efficiency. Provide examples of real-world applications where DES and AES are used.	***CO1***	***PO1***	**6**
			UNIT-III			
	4	a)	Find the results of the following, using Fermat's little theorem: a. 15^{15} mod 13 b. 15^{18} mod 17	***CO1***	***PO1***	**6**
		b)	State the Chinese Remainder Theorem and find X for the given set of congruent equations $X \equiv 4 \bmod 5$, $X \equiv 10 \bmod 11$.	***CO1***	***PO3***	**8**
		c)	Using quadratic residues, solve the following equation: $x^2 = 4 \bmod 14$	***CO2***	***PO2***	**6**
			UNIT-IV			
	5	a)	Differentiate between symmetric-key and asymmetric-key cryptosystems.	***CO1***	***PO1***	**6**
		b)	Find the value of 'd' and perform decryption and encryption using RSA algorithm with p=7, q=13, e=7 and Message=10.	***CO1***	***PO1***	**6**
		c)	In ElGamal, given the prime p = 31: a. Choose an appropriate e1 and d, then calculate e2. b. Encrypt the following messages "H", "E" , "L"; use 00 to 25 for encoding.	***CO2***	***PO2***	**8**
			OR			
	6	a)	Consider an elliptic curve $E_{11}(1,1)$ over a finite field 11. The generator point G is (6,6) . Assume that the private value n = 2. 1) Find the equation of the curve. 2) Find at least five points on the curve	***CO1***	***PO1***	**12**
		b)	Define a cryptographic hash function. Illustrate the working of message digest creation in SHA-512 with neat diagram.	***CO1***	***PO1***	**8**
			UNIT-V			
	7	a)	Identify and explain the types of attacks on digital signatures. provide a specific example scenario that illustrates how the above attack could be carried out on digital signatures.	***CO1***	***PO1***	**6**

SUPPLEMENTARY EXAMS 2024

		b)	A Tech company experienced a security breach where their encrypted communication channel was compromised. This resulted in the unauthorized access and exposure of confidential company data. Investigate how an attacker could have executed a man-in-the-middle (MitM) attack against the Diffie-Hellman key exchange to gain access to this sensitive information with neat diagram.	***CO1***	***PO1***	**8**
		c)	Create a neat diagram that clearly illustrates the structure of an X.509 certificate. Label each part of the certificate and briefly describe its purpose.	***CO2***	***PO2***	**6**

******

SUPPLEMENTARY EXAMS 2024